AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Beyond Afghanistan: Effective Combined Intelligence, Surveillance and Reconnaissance Operations

by Royce Frengle, Major, USAF

A Research Report Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements

Advisor: LTC Thomas Fife

Maxwell Air Force Base, Alabama
April 2010

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Table of Contents

Page

Abstract

Since the creation of the International Security Assistance Force (ISAF) in 2001, there has been tension between the US led Operation Enduring Freedom and the NATO led ISAF. Because of differing chains of command, levels of classification and systems, there was a lack of unity of effort in the Intelligence, Surveillance and Reconnaissance (ISR) collection operations. With the growth of all military forces in Afghanistan, there has been a reorganization to put all conventional forces operating in Afghanistan under the ISAF Joint Command. Collection management for conventional forces in Afghanistan is now conducted by the ISR Division (ISRD) within the IJC and sets the stage for more effective and efficient use of ISR collection platforms. However, there still exist some long term problems which hinder coalition ISR operations that must be addressed by both the US and its allies. Training and exercises need to be developed which build knowledge and experience in coalition ISR operations. Interoperability is the key to multinational military operations. As such, ISR platforms, data and processes need to meet international agreed upon standards. US personnel also need to overcome a cultural bias that favors unilateral ISR operations and accept that coalition operations are likely to continue to dominate future military operations. By addressing these long term issues, coalition ISR operations can become more efficient and effective in ISAF's Afghanistan operations and future multinational operations.

INTRODUCTION

In the early morning hours of April 17, 2009, the ground began to rumble beneath Nangarhar province in eastern Afghanistan as a magnitude 5.5 earthquake hit the region. Two hours later, a second earthquake of a 5.1 magnitude hit the region again. By the time the sun rose that morning, it was clear at International Security Assistance Force (ISAF) headquarters in Kabul that something should be done to help the Afghan people affected by this calamity. ISAF, Afghan government and Non-governmental organizations (NGO) all wished to provide aid but they did not have good information on what areas were most devastated by the earthquake. At the US national level and at US Central Command (CENTCOM), they tasked RQ-4 Global Hawk and satellites to image the region looking for damage. At ISAF Headquarters, they were unaware of the US imagery intelligence requests that had been put in. They also realized that if US systems took the images it would take from hours to days before they would be disseminated to the multiple customers that needed them at ISAF Headquarters. Additionally, in order to share those images with the host Afghan government would require contacting the producers of the images and requesting declassification. Declassification and foreign disclosure is not a quick process. In order to get a product for ISAF and Government of the Islamic Republic of Afghanistan (GIRoA) use quickly, the ISAF Intelligence Collection Coordination and Intelligence Requirements Manager (CCIRM) tasked his own collection assets, German Tornado reconnaissance aircraft based at Mazar-E-Sharif. Ultimately by the end of the day, both ISAF and GIRoA had the images that would aid them in allocating relief supplies but both ISAF and the US had separately tasked Intelligence Surveillance and Reconnaissance (ISR) collection assets to fill essentially the same requirement.

The problems associated with intelligence collection on this one event are indicative of the difficulties faced on a daily basis in providing ISR for combat operations in Afghanistan. In a counterinsurgency fight, effective intelligence drives operations.[1] Intelligence is also key to giving the commander an overall understanding the status of the insurgency in order to evaluate progress, reallocate resources, and plan future operations. The scarcity of intelligence collection assets demands that they are both efficiently and effectively used in a synergistic manner to meet the requirements of both the commander and subordinate commands. While there have been recent changes in the US and ISAF intelligence collection organizations to improve unity of effort there are still enduring issues with US and coalition ISR collection in Afghanistan. These issues can be mitigated through improved training, integration and a change in mindset by the parties involved in the process.

BACKGROUND

In order to understand the ISR operations in Afghanistan it is important to recognize who all the actors are and their relationship to each other. One of the most important concepts that most people do not realize is the extent to which Afghanistan operations are combined. In fact, until recently US forces did not make up the majority of the total foreign military forces operating in Afghanistan.[2] However, when it comes to ISR, the US has a large propensity of assets as well as the personnel trained to effectively manage them.

Until the fall of 2009, there were two different organizations responsible for intelligence collection for the entirety of Afghanistan. At ISAF HQ, in the CJ2, there was the Collection Coordination and Intelligence Requirement Management (CCIRM) shop. This organization was multinational but was plagued by a lack of trained personnel. CCIRM was responsible for

managing intelligence requirements, intelligence collection requests and requests for information from all of the regional commands except the US dominated Regional Command – East (RC-E) and requirements generated within the ISAF HQ. CCIRM had tasking authority over its own ISR assets which included Tactical Reconnaissance (TACRECCE) aircraft as well as Unmanned Aerial Vehicles (UAVs) operated by Italy and France.[3] For collection requirements that it could not satisfy, CCIRM could reach back to the NATO Intelligence Fusion Center (IFC) at RAF Molesworth, UK. CCIRM also sent unfilled requirements to the Joint Intelligence Operations Center- Afghanistan (JIOC-A) to be forwarded up to be filled by Combined Air Operations Center (CAOC) or CENTCOM assets.[4]

The other organization responsible for collection management in Afghanistan was the JIOC-A collection management shop. JIOC-A is a CENTCOM organization and supported not only unfilled ISAF collection requirements but also supported US national requests as well as Operation ENDURING FREEDOM (OEF) requirements. The US dominated RC-E also went directly to JIOC-A for its ISR collection requirements as they operated on the same systems and the same security/classification level as JIOC-A. While JIOC-A did not have any of its own ISR assets, it had directive authority for US MQ-1 Predator and MQ-9 Reaper UAVs. JIOC-A had direct ties to US intelligence agencies such as the National Security Agency (NSA), Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), and National Geospatial Intelligence Agency (NGA). JIOC-A did not suffer the same manning and training shortfalls as the CCIRM as it was easier for them to access trained US personnel. As a result of two organization doing very similar tasks but in different facilities, operating at different classification levels and on different systems, there was a lot of redundancy, lack of visibility

between what ISAF and US assets were tasked to collect. These problems were identified, but it took a larger organizational change within ISAF for a solution to be devised.

ISAF's scope and responsibilities have increased significantly since NATO assumed responsibility for command, control, and coordination of the ISAF in 2003. ISAF forces had grown from less than 20,000 in 2003 to over 60,000 in August of 2009. In response to the growth of the ISAF mission and forces, the ISAF HQ underwent a major reorganization in the fall of 2009. ISAF HQ remained in Kabul headed by a 4-star general, currently GEN Stanley McCrystal. This headquarters' mission changed to focus primarily on strategic political-military aspects of the ISAF mission and synchronizing ISAF's operations with the Afghan government and international organizations. A new 3-star command called the ISAF Joint Command (IJC) was created and headquarted at the Kabul International Airport. IJC will be responsible for executing day-to-day tactical operations throughout the country. The five regional commands, provisional reconstruction teams and theater enablers fall under the command of the IJC.[5]

The ISAF reorganization had major implications for theater intelligence collection management in Afghanistan. The personnel and responsibilities that we part of JIOC-A collection management and ISAF CCIRM were combined under the IJC CJ2 Intelligence Surveillance and Reconnaissance Division (ISRD). The ISRD solved many of the problems that existed prior to the reorganization. Unity of effort, requirements and asset visibility, and manning were all improved. The new shop expanded its organization to have ISR plans, current operations, requirements and assessments branch. The ISRD operates on ISAF Secret, SIPRNET and JWICS systems to ensure that it has access to the ISAF and US customers as well as the ability to access CAOC, CENTCOM and US national organizations. The ISRD does not have multinational manning like the ISAF CCIRM used to have. In fact they moved two non-

FVEY NATO personnel out of the ISRD when JIOC-A and CCIRM merged.[6] The ability to have LNOs for the ISAF collection assets was sacrificed to allow for access to US and FVEY classified systems.[7] Currently the ISRD is manned 80% by Americans with the remainder of the staffing coming from the United Kingdom and Canada.[8] While many problems were solved with the creation of the ISRD and the IJC, there still remain training shortfalls, a lack of interoperability and cultural differences between the US and other nations in the conduct of ISR operations.

TRAINING

There are several training concerns that need to be addressed both by the US and ISAF coalition partners. These training issues center on intelligence collection management and an understanding of the Tasking, Collection, Processing, Exploitation and Dissemination (TCPED) process. Training shortfalls occur at nearly every level from CENTCOM to the IJC down to the customers in the field. Some of the training shortfalls have been identified and CENTCOM is putting together Mobile Training Teams to deploy to Afghanistan and train forces in the field.[9] This is good start as a stopgap measure but a more comprehensive holistic approach needs to be taken.

Many countries contribute intelligence personnel to the ISAF mission in Afghanistan yet the level of training varies greatly. It is also not uncommon for someone outside the intelligence career field to fill intelligence billets. Even at the ISAF Joint Intelligence Centre, the senior intelligence analyst for RC-South was not a seasoned analyst but rather a ship's engineer from the Canadian navy.[10] The level of knowledge and experience of people filling intelligence positions vary greatly from country to country and within countries. Some country's intelligence

personnel have great analytical skills and possess a wide variety of HUMINT sources, yet they have little or no experience working with airborne ISR assets. Yet if they work in a large multinational mission such as that found in ISAF and don't understand the ISR platform capabilities and the TCPED process then they are at a severe disadvantage and put the forces they are supporting at an increased risk.

Since ISAF is formed around the core of NATO forces, NATO has taken on the responsibility of training forces for their deployment to Afghanistan. Academic training takes place at the NATO School in Oberammergau, Germany and the Joint Warfare Centre in Stavanger, Norway hosts mission rehearsal exercises for forces deploying to Afghanistan. The only course that the NATO school currently offers on intelligence for personnel deploying to Afghanistan is the ISAF Intelligence Orientation Course. This five day course is designed for personnel filling the ISAF CJ2 and as a secondary training audience the Regional Command and Provincial Recovery Team (PRT) J2 personnel. The course includes an overview of the current situation, CJ2 organization, fundamentals of analysis, Intelligence Preparation of the Battlespace (IPB), CCIRM, intelligence planning and counter-intelligence and HUMINT.[11] The short nature of the course and the number of topics to be covered preclude sufficient discussion on ISR collection management, platform capabilities and TCPED.

Since intelligence is a joint function in multi-national operations, NATO should take the lead and develop and offer a course in ISR operations. This course would help educate a multi-national training audience in ISR platform capabilities, the TCPED and ISR collection management principles. While a short course may not offer everything an intelligence student needs to know, it would at least set a baseline foundation of knowledge which could be built upon for specific military operations. Likewise, all NATO joint training events should include

realistic training to include planning and execution of ISR assets. If NATO does not provide adequate education and training on ISR, how can it expect success in conducting multi-national operations? Relying solely in the United States is not the answer.

The Unites States leads the world in its ability to plan and execute ISR operations. In recent years, we've grown from being able to not just effectively manage a single service's ISR platforms but to synchronize and cross-cue joint ISR assets, including national assets. Air Force intelligence is regarded as the experts in ISR collection and operations yet even within that community there exist training shortfalls. There is little formal training for Air Force intelligence officers in conducting intelligence in a multi-national environment. Neither the intelligence officer basic course nor the advanced Intelligence Master Skills Course provides any significant instruction on working with other countries. Part of the problem may exist because a culture has existed within the intelligence community of secrecy and an 'US Only' mentality. In recent years, presidential directives have forced intelligence to become more open in sharing of intelligence information with other countries, but the preexisting culture is slow to change.[12]

Training syllabi have also been just as slow to change. Currently many of the personnel in the ISRD receive pre-deployment training at the USAF Intelligence, Surveillance and Reconnaissance Operations Course (IROC) taught at Goodfellow AFB, Texas.[13] This course is the premier course for ISR operations within the DoD, yet it only provides a cursory discussion of coalition ISR ops (especially out of the 5-eyes community). Rather than an in-depth discussion of coalition ISR assets and their corresponding TCPED process, the students receive only basic information on platforms. For example, instruction may be as short as "This is Tornado, it is from by the UK, Germany and Italy.[14] It performs TACRECCE." This course is

supposed to qualify individuals to conduct collection management at a CAOC or JTF yet most of the knowledge they need about coalition ISR must be learned on the job.

An academic understanding of ISR assets and their associated TCPED provides a baseline for multinational ISR employment but to have a full mission capability multi-national ISR operations need to be exercised regularly. There are many bi-lateral and multinational exercises that the United States military participates in that could include realistic multi-national ISR operations. Most of the European countries as well as many other industrialized countries have modern airborne ISR assets with which they could participate. The US also has intelligence sharing agreements with many of the countries it exercises with, either as part of an alliance or unilaterally that could also be included in exercises. Some of the major exercises that provide a good training environment for multi-national ISR are Ulchi Freedom Guardian (US/South Korea), Freedom Resolve (US, Gulf Cooperation Council), Cobra Gold (US, Thailand) and Juniper Cobra (US/Israel). All of these exercises include a combined command post exercise and a field or live-fly exercise. This allows for both planning and executing combined ISR operations.

Education and training will provide US and allied forces the ability to better conduct combined ISR operations. This knowledge and experience can be applied to the current fight in Afghanistan or to future coalition operations. Education and training can definitely improve airborne ISR effectiveness and efficiency but there must also be significant growth in ISR systems interoperability.

INTEROPERABILITY

Interoperability refers to the ability of different military organizations to conduct joint operations. Those organizations can come from different countries or different services within a country. Interoperability allows forces to operate together by sharing common doctrine, procedures and resources and most importantly it allows them to communicate together.[15] Interoperability forms the core of modern joint and combined operations. In today's resource constrained environment, interoperability allows commander's to make the most of forces assigned to them. Since ISR systems are in high demand in the current fight in Afghanistan, interoperability is a major key to maximizing the utility of those assets.

As a long standing and strong military alliance, NATO has gone through great pains to ensure interoperability of the 28 member nations. NATO's measures for interoperability have been adapted by many other non-NATO countries who want to be able to integrate into operations with NATO countries. Implementing interoperability is done through NATO Standardization Agreements commonly known as STANAGs. There are hundreds of STANAGs that govern everything from language proficiency to ammunition standardization. While STANAGs help ensure interoperability, stovepiped and proprietary systems and data hinder the effectiveness and efficiency of ISR.

Some of the lack of interoperability is a result of the rapid deployment of ISR aircraft by ISAF troop contributing nations to help alleviate the chronic shortage of airborne ISR. With the growth of ISAF forces, the increase in operations has highlighted the need for more intelligence. NATO has a standing urgent need request out to the ISAF troop contributing nations for additional ISR assets. The national contributions are honorable, but the manner in which they are deployed can limit their usefulness. When a country deploys airborne ISR assets to Afghanistan, they must choose who will have tasking authority over that platform. That is,

whose intelligence requirements the platform will be attempting to satisfy. There are three common ways they can task ISR platforms, through national chains, through ISAF or through the CAOC. Under national tasking, a country's ISR platform will only satisfy the ISR requirements of that country's forces. This method is effective (for that country) and interoperability is not required. This method however is not efficient as it does nothing to satisfy the ISR requirements of other forces in Afghanistan. Nations can also deploy ISR assets under ISAF's operational control. This method is more flexible and efficient because the systems will usually be tasked against ISAF's highest priority collection requirements. However, if they are not fully interoperable with all the ISAF contributing nations, they have limited effectiveness. Nations frequently choose ISAF control because they want to be seen as supporting the whole ISAF mission but don't want to put their assets under the US controlled CAOC. The final common method for control is to put assets under the CAOC-CENTCOM to be tasked by the CAOC's ISRD. This is how the USAF and some of the USN put all their theater ISR assets. This is an effective and efficient method that works well for FVEY countries since they can actively manage their assets because most of the operations at the CAOC operate at the releasable to FVEY classification level.

We see that the tasking authority and security classification affect the level of interoperability we can see where some of the problems arise. Nations generally acquire and develop military systems for their national use, rather than for use within a coalition. This does not usually become a problem when assets are tasked under national authority, however it does cause complications when assets are tasked by ISAF or the CAOC. Part of the interoperability issues are because the TCPED is done on systems that are not connected to the networks that most forces in Afghanistan have (ISAF SECRET or SIPRNet). Other issues arise because data

cannot be disseminated to forces because the ISR platforms don't have the correct communications or datalink systems. For example, when the French Harfang UAV was initially deployed to Afghanistan in early 2009, it was unable to directly downlink its FMV feed to units in the field because it lacked the ROVER (Remote Optical Video Enhanced Receiver) downlink capability. The ROVER downlink is not a NATO approved datalink and the US has placed export restrictions on the equipment it uses. However, when forces comply with NATO standards, there is significant value added. The French Harfang detachment deployed to Bagram did not have a GMTI analyst although the UAV had a GMTI capability, but because the GMTI data meet NATO standards they were able to give the post mission GMTI data to the RC-E CJ2 section and an US army military intelligence specialist was able to analyze it. This is an excellent example of how the benefits of interoperability pay dividends in coalition ISR operations.

Because the need to field new ISR systems is so great, most of the effort is put into rapidly fielding and deploying a capability rather than determining how that capability can practically be used and how the TCPED cycle will incorporate into larger national and theater processes. These 'science projects' often start with a good idea but generally lack the time consuming discussions on how to sustain and integrate the system. The ROVER capability is a good example of a system that has been very effective but was a result of ad-hoc adaptation rather than a deliberate capability that was compliant with NATO standards. The ROVER capability was really an adaptation of an unused LOS control link on the MQ-1 Predator that could downlink the video directly off the aircraft. This capability was soon adapted so that fighters and bombers with advanced targeting pods could also downlink video and a large number of ROVER ground stations were deployed to US and coalition ground forces and

JTACs. While ROVER has been very successful in combat by giving ground forces the eagle eye perspective, it does not meet interoperability standards for NATO.

Since 2005, NATO has published the NATO ISR Interoperability Architecture (NIIA) document which spells out exactly how ISR information will be collected and shared. The NIIA also gives 14 STANAGs which spell out the details how each of the type of intelligence data will be formatted and transmitted.[16] An example of one of these STANAGs is STANAG 4586 *UAV Control System Architecture*. This 250 page document which spells out the different levels to which UAV systems will be interoperable and how the intelligence they gather will be shared with different ground stations.[17] These STANAGs are important because they move away from inflexible stovepipe systems that use proprietary sensor and UAV control streams towards a more open architecture that promotes sharing of data to build synergies and effectiveness. The U.S. Army has used the STANAG 4586 as a basis for their 'One System' UAV ground control station. This single station can control the RQ-7 Shadow, RQ-5 Hunter and the MQ-1C Sky Warrior. With little modification this ground control station can fly and receive data from any US or coalition UAV that is compliant with STANAG 4586.[18] Even the newest versions of the ROVER ground terminal have begun to be able to receive data from STANAG compliant UAV video feeds.[19] The increasing proliferation of interoperable systems will significantly aid in improving coalition ISR by creating an open architecture with which systems from any nation can feed information.

The US has moved in the right direction in upgrading existing ISR collection systems to be more interoperable with joint and coalition partners. There are some existing problems that still need to be resolved. There are still many ISR 'science projects' that are developed and put into the field to meet a perceived urgent need that are not interoperable with existing systems or

lack a developed TCPED cycle. Often these 'science projects' are put into a theater to prove a concept or technology that will help counter improvised explosive devices or other threat which challenges existing collection capabilities. Decision makers need to step back and take a more holistic approach to putting ISR collection assets into theater. An ISR system that is integrated into existing TCPED processes and interoperable with other joint and coalition systems is much more effective and can be efficiently used without the pains associated with 'drive-by fielding'.

One of the final elements of the interoperability that continues to be a problem in coalition ISR operations is the use of different computer systems. This problem is generally arises in the tasking of ISR assets dissemination of intelligence products. If ISAF forces in the field need ISR support they will normally have submit a request on either their national or ISAF Secret classified computer networks. If the ISR request is going to be satisfied by a US ISR asset, at the regional command or IJC level those requests will have to be either physically or electronically transferred to SIPRNET or JWICS. The collection, processing or exploitation will be done on SIPRNET or JWICS system, and the final product will have to be transferred back to the national or ISAF system for dissemination. The physical or electronic transfer of requests and products creates a lot of friction and additional time to complete the TCPED process.

ADDITIONAL ISSUES

There are additional issues that exist beyond training and interoperability which hinder joint intelligence operations in Afghanistan. These issues are a little more difficult to grasp since their roots are cultural. The United States and the role it plays in multinational military operations is also a central issue.

A predominate aspect of military culture has developed in the United States military at all levels that has downplayed the importance of multinational operations and has favored a unilateral approach. The lack of trust and cooperation with allied countries has existed for a long time; there are many examples of this during World War II.[20] It is easy to understand why this avoidance of multinational operations exists. Many of the benefits of multinational operations can only be seen at the strategic and political levels of war. Some of the examples seen at this level include alternate perspectives on regional issues, cultural understanding and political legitimacy. Of course there are benefits at the operational level which include an increase in overall capabilities, niche capabilities and operational and tactical experience. On the flip side, there are many challenges with coalition operations which are evident at tactical and operational level. Most Americans see confused chains of commands, difficulty communicating, differing ROE and other problems that make daily operations more difficult and frustrating. Also these issues take away from unity of effort. As military members grow up dealing with all the issues with coalitions at the operational and tactical levels, it shapes their view as they grow into more senior positions. This leads to an attitude that it is just easier and more efficient to conduct unilateral operations.

To overcome this cultural roadblock the US needs to make sure its military personnel are aware of the reasons, advantages, and challenges of multinational operations. Mutual confidence is essential when working in a multinational environment. To build this mutual confidence, we need to provide opportunities to build rapport with foreign military personnel, learn respect for our differences, educate our forces about our partners, and be patient.[21,22] Building strong working relationships takes time. Multinational military operations are difficult. Our military

and political leaders must realize when they should go through the pains of multinational operations and when it is best to go it alone.

The US leads the world in technologically advanced intelligence collections platforms and enterprises. Our love of technology combined with the aversion to working with other countries, combines to lead to reluctance to embrace the intelligence collection capabilities of other countries. The reluctance to accept and integrate foreign ISR platforms into our operations is a significant problem in integrating other capabilities into a US dominated operations. A tendency to overlook the contributions other countries can alienate our partners and erode mutual confidence between our militaries. Our allies also need to realize that they need to remain actively involved in multinational operations. They cannot allow an attitude to develop that the US will take care of everything. By having allies actively involved in a leadership role, we will have a counterbalance to our views and additional military options might be brought to the table that the US military might not develop alone.

CONCLUSION

Today's coalition ISR collection efforts in Afghanistan have made significant improvements within the last year. The creation of the ISAF Joint Command and the Intelligence, Surveillance and Reconnaissance Division has done much to enhance the unity of effort of US and ISAF collection management. These recent organizational changes should be viewed with some skepticism for ISAF was created in December 2001 and has conducted operations since 2003.[23] The fact that it took nearly eight years for a significant reorganization does not bode well for the other longer-term changes that need to take place for coalition ISR operations to be more effective and efficient. Yet we must not lose sight of the long term goal to improve coalition ISR. Training and exercises will build knowledge and experience into the

intelligence professionals that will manage future intelligence collection operations. Interoperability of current and future intelligence and information management systems is critical as the rapid flow of information becomes more and more essential to mission success. More and more we need to become aware of the cultural differences between us and our allies and work around those to ensure that we are all focused on the same mission.

If we do not focus more effort on improving our coalition ISR operations, we not only doom ourselves to ineffective and inefficient ISR for our operations in Afghanistan but put risk on future coalition operations. Next time our vital national interests may be at stake and our adversary won't give us years to get our ISR operations right.

1. FM 3-24, *Counterinsurgency*. pg 1.23
2. ISAF Official Website, "ISAF Placemat".
3. This paper is written for a joint and combined audience, therefore the term UAV is used rather than the USAF term Remotely Piloted Aircraft (RPA)
4. Author's experience while deployed from Nov 2008-May 2009
5. ISAF Official Website, "ISAF Command Structure".
6. Mr. Warren LePine, Intelligence Requirements Manager, ISRD, IJC, Kabul, Afghanistan, to the author, e-mail, 21 March 2010.
7. 5-Eyes countries include United States, United Kingdom, Canada, Australia, and New Zealand
8. Lt Col Jason Green, ISRD, Deputy Chief, IJC, Kabul Afghanistan, to the author, e-mail, 25 February 2010.
9. Ibid.
10. Author's experience while deployed from Nov 2008-May 2009
11. NATO School, "ISAF Intelligence Orientation Course Description", May 2007.
12. The actual presidential directive remains classified but a majority of the directive focuses on intelligence sharing with the FVEY countries.
13. Lt Col Jason Green, ISRD, Deputy Chief, IJC, Kabul Afghanistan, to the author, e-mail, 25 February 2010.
14. Maj Tim Lucas, IROC student, Jan-Feb 2010, to the author, e-mail, 28 February 2010.
15. NATO, Backgrounder: Interoperability for joint operations, July 2006.
16. NATO Standardization Agency, Allied Engineering Documentation Publication AEDP-02: NATO Intelligence, Surveillance and Reconnaissance (ISR) Interoperability Architecture (NIIA), September 2005.
17. NATO, Backgrounder: Interoperability for joint operations, July 2006.
18. Defense Industry Daily"It's Better to Share: Breaking Down UAV GCS Barriers", 16 March 2010.
19. L3 Communications, Brochure for ROVER 5 Handheld Device, 4 June 2008.
20. One of the example is the relationship between General Patton and Field Marshall Montgomery
21. NATO Allied Joint Publication AJP-3(A) Allied Doctine for Joint Operations (ratification draft), 2006, pg 1-18.
22. Joint Publication (JP) 3-16, *Multinational Operations*, 7 March 2007, p.I-3.
23. ISAF Official Website, "ISAF History".

APPENDIX: Abbreviations and Acronyms

CAOC – Combined Air Operations Center

CCIRM – Collection Coordination and Intelligence Requirements Management

CENTCOM – United States Central Command

CIA – Central Intelligence Agency

CJ2 – Combined Joint Directorate of Intelligence

DIA – Defense Intelligence Agency

FVEY – Five Eyes (United States, Canada, United Kingdom, Australia, New Zealand)

GIRoA – Government of the Islamic Republic of Afghanistan

GMTI – Ground Moving Target Indicator

HUMINT- Human Intelligence

IFC – Intelligence Fusion Centre

IJC – ISAF Joint Command

IMINT – Imagery Intelligence

IPB – Intelligence Preparation of the Battlespace

IROC – ISR Operations Course

ISAF – International Security Assistance Force

ISR – Intelligence, Surveillance and Reconnaissance

ISRD – Intelligence, Surveillance and Reconnaissance Division

JIOC-A – Joint Intelligence Operations Center- Afghanistan

JTF – Joint Task Force

JWICS – Joint Worldwide Intelligence Communications Systems

JTAC – Joint Terminal Attack Controller

LNO – Liaison Officer

MTT – Mobile Training Team

NATO – North Atlantic Treaty Organization

NGA – National Geospatial Intelligence Agency

NGO – Non-Governmental Organization

NSA – National Security Agency

OEF – Operation ENDURING FREEDOM

PRT – Provincial Reconstruction Team

RC-E – Regional Command – East

ROVER – Remote Optical Video Enhanced Receiver

SAR – Synthetic Aperture Radar (imagery)

SIGINT – Signals Intelligence

SIPRNet – Secure Internet Protocol Router Network

STANAG – NATO Standardization Agreement

TACRECCE – Tactical Reconnaissance

TCPED – Tasking, Collection, Processing, Exploitation and Dissemination

UAV – Unmanned Aerial Vehicle

UK – United Kingdom

BIBLIOGRAPHY

Field Manual (FM) 3-24, *Counterinsurgency*, December 2006.

Defense Industry Daily, "It's Better to Share: Breaking Down UAV GCS Barriers", 16 March 2010. http://defenseindustrydaily.com

ISAF Official Website, "ISAF Command Structure". http://www.isaf.nato.int/en/isaf-command-structure.html (accessed 10 March 2010)

ISAF Official Website, "ISAF History". http://www.isaf.nato.int/en/our-history/ (accessed 10 March 2010)

ISAF Official Website, "ISAF Placemat". http://www.isaf.nato.int/en/isaf-placemat-archives.html (accessed 7 November 2009)

Joint Publication (JP) 2-0, *Joint Intelligence*, 27 June 2007.

Joint Publication (JP) 3-16, *Multinational Operations*, 7 March 2007.

NATO Allied Joint Publication AJP-3(A) Allied Doctine for Joint Operations (ratification draft), 2006

NATO, Backgrounder: Interoperability for joint operations, July 2006. http://www.nato.int/docu/interoperability/interoperability.pdf (accessed 3 March 2010)

NATO School, "ISAF Intelligence Orientation Course Description", May 2007. http://www.natoschool.nato.int/new_www/courses/POIs/P2_23.htm (accessed 11 February 2010)

NATO Standardization Agency, Allied Engineering Documentation Publication AEDP-02: NATO Intelligence, Surveillance and Reconnaissance (ISR) Interoperability Architecture (NIIA), September 2005.

L3 Communications, Brochure for ROVER 5 Handheld Device, 4 June 2008. http://www.L-3com.com/csw